



Internet and Email Acceptable Usage Good Practice Guide

August 2009



contents

<u>1</u>	<u>Introduction to Good Practice Guides</u>	<u>3</u>
<u>2</u>	<u>Acceptable Internet and Email Usage Overview</u>	<u>3</u>
<u>3</u>	<u>Acceptable Internet Usage Good Practice Guidelines</u>	<u>3</u>
<u>4</u>	<u>Email Usage Good Practice Guidelines</u>	<u>6</u>
<u>5</u>	<u>Appendix A: Definitions</u>	<u>10</u>
<u>6</u>	<u>Appendix B: Checklists</u>	<u>10</u>
6.1	Good Practice Checklist	10
<u>7</u>	<u>Document Control</u>	<u>13</u>

1 INTRODUCTION TO GOOD PRACTICE GUIDES

This document is a good practice guide concerning acceptable use of the Internet and Email in relation to computer and network resources within the various international agricultural research centers that are supported by the Consultative Group for International Agricultural Research (CGIAR). This guide forms part of the CGIAR-wide baseline ICT Security and Acceptable Use good practice set. The target audience for the good practice guides are all centers affiliated with CGIAR, and in particular, the IT teams within each center.

The good practice set does not contain mandatory requirements that centers are required to implement. Instead, it outlines a number of good practices with respect to enterprise ICT security and acceptable use. The prudence of implementing specific good practices identified in this guide will depend on the risk profile associated with the ICT environment in each center. A set of checklists is provided at the end of this guide to assist with the process of determining those good practices which will be relevant depending on the risk profile of each center.

The initial ICT Security and Acceptable Use good practice set has been prepared in consultation with the CGIAR center IT community under a process jointly managed by the CGIAR ICTKM Program and the CGIAR Internal Auditing Unit (IAU). This guide draws on the results of work undertaken in the CGIAR Enterprise Security and Business Continuity Project; additional inputs from the IT community, internal auditors, and from SIFT Pty Ltd, an information security and risk management services firm which assisted in the preparation of these guides. The ICTKM and IAU units will coordinate future updates in consultation with the CGIAR center IT community.

2 ACCEPTABLE INTERNET AND EMAIL USAGE OVERVIEW

The Internet provides access to an array of information, resources and services that provide potential opportunities and benefits which aid and support the work of CGIAR research centers. However, if staff do not use the Internet responsibly, it can expose those centers to risks at both a technical level (with potential damage being caused to ICT infrastructure) and an operational level (with misuse of Internet resources leading to possible reputational damage to centers and a loss in productivity).

These guidelines establish a set of good practices for acceptable use that staff in CGIAR centers should adhere to when using the Internet within centers.

3 ACCEPTABLE INTERNET USAGE GOOD PRACTICE GUIDELINES

It is recommended that CGIAR centers should maintain Internet good practice guidelines for staff to adhere to when using the Internet within the centers. This document should be distributed to all users in the relevant CGIAR center.

Downloading

- 3.1.1 CGIAR centers should make clear to staff, through orientation materials, network user guides and other permanently available information, that before any information is downloaded, a staff member should:
- Check the legality of downloading the information, particularly with respect to copyright permission. If in doubt of the legality, staff members should contact the Center focal point on IP matters for advice.
 - Be aware that many Internet sites maintain records of who accesses (or visits) them and what, if anything, they download from the site.

- Not redistribute downloaded material unless the owner has given permission for them to do so either directly or in the copyright/license terms.
- Not download unlicensed software or violate limitations on the use of particular software as imposed by any licence agreements. Most downloaded software, including shareware and freeware, is copyrighted and subject to license, which sets limitations on its use.
- Before installing downloaded software on their center workstations, first verify that the software has been obtained from a reputable source and virus scan any downloaded files prior to installation.

3.1.2 Systems that are used to conduct "secure" or "sensitive" activities as part of the work of a center (for example, financial or banking transactions) should not also be used for other activities (such as research) which may require the installation of arbitrary software applications (including those downloaded from the Internet).

Prohibited and Permitted Usage

3.1.3 CGIAR Centers should make clear to staff, through orientation materials, network user guides and other permanently available information, what comprises prohibited usage from center provided connections to the Internet. These prohibitions would typically include the following:

- Conducting an external business enterprise or political activity; engaging in any form of intelligence collection from center facilities; engaging in fraudulent activities; or knowingly disseminating false or libelous information.
- Misusing, disclosing without proper authorisation, or altering personnel information (e.g., making unauthorized changes to personnel files, or sharing personnel data with unauthorized parties).
- Any unauthorized, deliberate action that damages or disrupts computing systems or networks; alters their normal performance, or causes them to malfunction.
- Wilful or negligent introduction of computer viruses, Trojan horses or other destructive programs into center systems or networks or into external systems and networks.
- Unauthorised decryption or attempt at decryption of any system or user passwords or any other user's encrypted files.
- Packet sniffing, packet spoofing, or use of any other means to gain unauthorised access to information, a computer system, or network.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Any form of online gambling.
- Accessing pornography sites.
- Issuing statements or opinions on any subject on behalf of Center or on behalf of other individuals unless appropriately authorized to do so in accordance with Center external communications policies.
- Requesting, accessing, posting, or downloading of any material that incites crime or terrorism (as defined in either the receiving or hosting country, or any country through which the information is routed)

- 3.1.4 CGIAR Centers should make clear to staff, through orientation materials, network user guides and other permanently available information, the need, when issuing statements, comments or opinions on websites, blogs, forums and similar electronic venues, regarding of the importance of maintaining the corporate image of CGIAR and its affiliate centers. All statements, comments or opinions should therefore be expressed in a professional and non-offensive manner.
- 3.1.5 Incidental personal use of the Internet should only be permitted within CGIAR centers as long as it does not consume an excessive amount of time or bandwidth and does not interfere with an employee's official tasks.
- 3.1.6 CGIAR Centers should make clear in guidelines to staff that, in situations where they engage in e-commerce transactions for official purposes over the Internet, using corporate credit card or banking information, they should first ensure that the organisation with whom they are dealing is reputable and legitimate, and that such transactions can be completed in a secure fashion (for example, through use of SSL) .

Logging and Monitoring of Internet Usage

- 3.1.7 CGIAR centers should retain the right to be able to deny access to any ICT system and may examine or disclose online information that center ICT systems have been used to access according to established criteria. Such criteria would usually include the following circumstances:
- When required by and consistent with host country law
 - When the center has reason to believe that violations of law or of center policies are threatened or have taken place;
 - When there are compelling circumstances where failure to act may result in significant harm to the center, CGIAR generally or an individual associated with the center; or

Note that centers should maintain awareness of the legal, regulatory and compliance environments which surround workplace surveillance and monitoring in their respective host countries (including state or provinces where such level of regulation is in place). There may be restrictions in place or requirements that must be fulfilled prior to any examination or disclosure of information on a user's system.

Centers should establish procedures for accessing the email messages or website browsing of staff whereby this must be approved ex ante by a senior manager of the center, and preferably two senior managers to ensure that the established criteria for such access have been met, and that there can be no question by staff concerned of abuse of this procedure.

- 3.1.8 It is recommended that CGIAR centers log details of all Internet content that is accessed, including the following information:
- URL of content accessed
 - Time and date of access
 - User who accessed the content

The log file should contain records of content accessed in the preceding 90 days. In addition, backups of the log file should be performed regularly to ensure that content accessed in the past year can be reviewed by accessing these backups.

Transmission of Sensitive and/or Personal Information

- 3.1.9 CGIAR centers should make clear to staff, through orientation materials, network user guides and other permanently available information, that they should not use the Internet to send sensitive information belonging to the center (such as non-public research data or passwords used to gain access to systems and devices within a center) in unencrypted form. This includes the sending of sensitive information using any of the following means:

- E-mail
- Posting to newsgroups
- Posting to forums, blogs or websites

It should be made clear to users the importance of sending sensitive information with extreme caution; search engines may be able to index that information if it is not appropriately secured, which could potentially render it viewable and easily accessible by a large number of untrusted parties. Hence, if sensitive information does need to be sent over the Internet, if possible it should be sent after it has been encrypted. Examples of possible file encryption solutions include PGP (via email) and SecureZIP. Alternatively, the information can be transmitted through the use of protocols that use encryption such as Secure FTP.

- 3.1.10 CGIAR centers should make clear to staff, through orientation materials, network user guides and other permanently available information, that no responsibility is assumed by the organization for any of their personal information transmitted by them (such as for personal e-commerce transactions or banking transactions) using center provided Internet connections, including any consequential losses sustained as a result of the transmission of this information.

Filtering of Internet Access

- 3.1.11 CGIAR centers should retain the right to implement filtering of some or all Internet content accessed by its staff

4 EMAIL USAGE GOOD PRACTICE GUIDELINES

The email systems of CGIAR centers should be used primarily for research and business purposes. Hence, while some incidental personal use of email may be permitted by centers, this should not extend to allowing email usage that:

- Consumes an excessive amount of system resources;
- Interferes in any way with worker productivity;
- Places sensitive information or systems belonging to CGIAR centers at risk of compromise;
- Involves illegal activity or non-compliance with center codes of conduct or anti-harassment policies; or
- Pre-empts any research activity of CGIAR centers.

The guidelines in this section are designed to ensure that email usage in CGIAR centers occurs in a responsible and secure manner which minimises the risk of detrimental impact to centers themselves.

It is recommended that CGIAR centers maintain email good practice guidelines to be implemented by staff. This document should be distributed to all users in the relevant CGIAR center.

Content of Emails

- 4.1.1 CGIAR centers should make clear to staff, through email good practice guidelines that any information regarded as confidential or proprietary, including legal or contractual agreements, trade secrets, and any technical information related to the operations of a particular CGIAR center (or partners of centers) should not be communicated via email to external parties. In cases when confidential or proprietary information is required to be communicated through email, the use of encryption should take place.
- 4.1.2 Each Center should conduct a risk assessment to determine which data should not be communicated via email without encryption. More information about the use of encryption for transmission of sensitive data is provided in the CGIAR Internet Security Good Practice Guide.
- 4.1.3 To facilitate communications and to properly identify the sending party, it is recommended that all emails sent using CGIAR center email systems contain a signature that consists of, at minimum, the following:
- Sender's Full Name
 - Position Title
 - Center Name and Address
 - Email address
 - Web site URL of center
 - Phone and fax numbers (including relevant area codes)
 - An indication that the center is supported by the Consultative Group on International Agricultural Research

In addition, before any emails are sent, it is recommended that:

- The email is given an appropriate subject title which provides a concise and meaningful reference to the content of the email message
 - The email is only sent to recipients to whom the contents is relevant
 - Attachments are only included in the email if absolutely necessary and, if this is the case, consideration should be given to ensuring the attachment is in an appropriate format and of a manageable file size
- 4.1.4 It is recommended that any outgoing emails sent by users from CGIAR accounts to external non CGIAR users include a disclaimer similar to the following appended to the email via the email server:

IMPORTANT NOTICE – This email and the information that it contains may be confidential, legally privileged and protected by law. Access by the intended recipient only is authorized. Any liability (in negligence or otherwise) arising from any third party acting, or refraining from acting, on any information contained in this email / facsimile is hereby excluded. If you are not the intended recipient, please notify the sender immediately and do not disclose the contents to any other person, use it for any purpose, or store or copy the information in any medium. Copyright in this email / facsimile and attachments created by us belongs to <CENTER NAME>. <CENTER NAME> also asserts the right to be identified as such and object to any misuse.

Acceptable Use of Email

- 4.1.5 Centers should publish Acceptable Use of Email Policies, provided to new staff (and others receiving CGIAR email accounts) for their review and agreement, that include the following requirements:
- Users of CGIAR email systems should not send any information that incites crime (as defined in either the sending or receiving country, or any country through which the information is routed)
 - Email systems in CGIAR centers should not be used to produce or distribute “chain mail,” operate businesses, or make solicitations for personal gain, political or religious causes, or outside organizations. Users shall not forward or otherwise propagate, to individuals or groups, chain letters, pyramid schemes or any other types of data that may unnecessarily consume system resources or otherwise interfere with the work of others.
 - Email should not contain any material that is offensive, defamatory, or threatening to others. These may include statements, messages, or images consisting of pornographic material, ethnic slurs, racial epithets, or anything that may be construed as harassing, offensive, or insulting to others based on race, religion, national origin, color, marital status, gender orientation, citizenship status, age, disability, or physical appearance.
 - Users of CGIAR email systems should not email the configuration details of any networks or servers within CGIAR centers to public newsgroups or mailing lists. This includes internal machine addresses, server names, server types, or software version numbers.
 - Where business communications of CGIAR centers are sent via email, they should only be sent using official center email accounts.
 - It is recommended users of CGIAR email accounts not allow anyone else access to their account. However, in some situations, it may be necessary for this to occur. In such situations, access to another party’s email account should only occur where the person who owns the email account has provided a written request to the center IT manager (which has been approved). The request should:
 - Identify who the email account will be accessed by and how long this arrangement will be in place; and
 - Contain an acknowledgement by the owner of the email account that they will continue to be responsible for all activity on the account.
 - Access to email messages should be limited to properly authorized CGIAR personnel. Hence, staff within CGIAR centers should not share their email account passwords with other individuals in any circumstances.
 - Users of CGIAR email systems should not publish or distribute internal mailing lists to non-staff members. Internal mailing lists typically contain email accounts and addresses used to distribute email messages to all or a subset of CGIAR center staff.
 - Users should not forge, attempt to forge, disguise or attempt to disguise the user’s identity for email messages sent using CGIAR email systems.
 - Users of CGIAR email systems should not send unsolicited bulk mail messages using CGIAR center email systems. Users should also be made aware of and comply with any relevant laws which regulate the sending of bulk and ‘spam’ emails.
 - Use of personal web-based email accounts is permitted in CGIAR centers, however users should treat attached files and website links as potentially harmful and refrain from downloading or following either of these on CGIAR center desktops or laptops. CGIAR center users should not use personal email accounts for work purposes.

Email Accounts

- 4.1.6 Users of CGIAR email systems should not be permitted send email messages using another person's CGIAR center email account, unless special dispensation for this to occur has been provided in accordance with 4.1.5.
- 4.1.7 Individual email accounts provided to users of CGIAR email systems should identify users by their real name; pseudonyms that are not readily attributable to actual users should not be allowed. Note that this does not preclude the use of generic accounts such as "Help Desk" where required for business purposes.

Avoiding Malicious Email Content

- 4.1.8 Users of CGIAR email systems should be careful to not execute any untrusted programs on CGIAR systems that are received via either personal or center email accounts, nor should users install any software upgrades or patches received via these accounts.
- 4.1.9 It is recommended that users disable automatic previewing of HTML email messages in client software (display of messages should be set to "text only" by default). Automatic loading of pictures, as well as downloading and processing of active content within messages should be also disabled by default. These requirements may be waived if mitigating controls are in place such as anti-virus on both the mail gateway, and the end user's desktop.

5 APPENDIX A: DEFINITIONS

Email: The electronic transmission of information through a mail protocol such as Simple Mail Transfer Protocol (SMTP).

Encryption: The process by which data is re-arranged into an unreadable or unintelligible form for confidentiality, transmission or other security purposes

File Transfer Protocol (FTP): A standard Internet protocol that is used to exchange files between computers on the Internet. FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to download programs and other files to your computer from other servers.

Secure Sockets Layer (SSL): SSL provides a method of authenticating the communicating parties (client and server authentication) and encrypting the information exchange between those parties. SSL is supported by most web browsers and web servers.

Shareware: Software supplied on a 'try before you buy' basis. Shareware is produced by software companies and independent programmers and supplied to users through a variety of channels including magazine cover disks, e-mail, mail order, Internet downloads, etc.

6 APPENDIX B: CHECKLISTS

The following checklist is designed to assist CGIAR centers that wish to adopt any or all of the good and better practices listed in this document. The checklists should be used by a center when attempting to assess their level of current adherence with the guidelines listed in this document. This will allow any gaps with good practices to be identified, after which centers can assess whether addressing those gaps will be feasible.

6.1 Good Practice Checklist

Guideline Number	Guideline	Tick if center currently adheres to this guideline
Section 3 – Acceptable Internet Usage Good Practices		
Downloading		
3.1.1a	Center guidelines require that staff: <ul style="list-style-type: none"> ▪ Check legality of downloading information ▪ Be aware that Internet sites often maintain access records 	<input type="checkbox"/>
3.1.1b	<ul style="list-style-type: none"> ▪ Do not redistribute downloaded material unless owner grants express permission 	<input type="checkbox"/>
3.1.1c	<ul style="list-style-type: none"> ▪ Do not download unlicensed software and comply with license agreements for software. 	<input type="checkbox"/>
3.1.1d	<ul style="list-style-type: none"> ▪ Only download software obtained from reputable sources by staff and installed only after virus scan. 	<input type="checkbox"/>
3.1.2	Systems used for sensitive or secure activities not also used for other activities requiring installation of arbitrary software	<input type="checkbox"/>

Guideline Number	Guideline	Tick if center currently adheres to this guideline
	applications	
Prohibited and Permitted Usage		
3.1.3	Internet use guidelines cover the prohibitions listed in guideline 3.1.3	<input type="checkbox"/>
3.1.4	CGIAR center staff made aware of need to maintain corporate image when making statements/comments/opinions online.	<input type="checkbox"/>
3.1.5	Incidental personal Internet use permitted provided it does not involve excessive time or bandwidth consumption and does not interfere with official work tasks	<input type="checkbox"/>
3.1.6	Staff engaging in e-commerce transactions made aware to ensure they are dealing with a reputable and legitimate organisation	<input type="checkbox"/>
Logging and Monitoring of Internet Usage		
3.1.7	CGIAR centers retain right to deny access to ICT systems and may examine information ICT systems have been used to access in accordance with guideline.	<input type="checkbox"/>
3.1.8	Centers log detail of all Internet content accessed by its users	<input type="checkbox"/>
Transmission of Sensitive and/or Personal Information		
3.1.9	Staff do not send sensitive center information over Internet unless specific business purpose exists and recipient is a trusted party If sensitive information sent, encryption is used where possible	<input type="checkbox"/>
3.1.10	Staff informed that no responsibility is assumed by center for any personal information transmitted over center provided Internet connections	<input type="checkbox"/>
Filtering of Internet Access		
3.1.11	CGIAR Centers retain right to implement filtering of Internet content accessed by staff	<input type="checkbox"/>
Section 4.1 – Email Usage Good Practices		
Content of Emails		
4.1.1	Confidential/proprietary information not communicated via email, or if communicated, encryption used	<input type="checkbox"/>
4.1.2	Data which should not be communicated via email without encryption has been determined	
4.1.3	Emails include appropriate signature	<input type="checkbox"/>
4.1.4	Emails include appropriate disclaimer	<input type="checkbox"/>

Guideline Number	Guideline	Tick if center currently adheres to this guideline
Acceptable Use of Email		
4.1.5a	Center guideline requires that <ul style="list-style-type: none"> ▪ users do not send information via email that incites crime 	<input type="checkbox"/>
4.1.5b	<ul style="list-style-type: none"> ▪ Emails not used to produce/distribute chain mail/operate businesses etc. ▪ Users do not forward any emails/data that unnecessarily consume system resources 	<input type="checkbox"/>
4.1.5c	<ul style="list-style-type: none"> ▪ Emails do not contain offensive/defamatory/threatening material 	<input type="checkbox"/>
4.1.5d	<ul style="list-style-type: none"> ▪ Configuration details of CGIAR center networks/servers not posted to newsgroups/ mailing lists 	<input type="checkbox"/>
4.1.5e	<ul style="list-style-type: none"> ▪ Business communications sent using official CGIAR center email accounts 	<input type="checkbox"/>
4.1.5f	<ul style="list-style-type: none"> ▪ Users do not permit others to access their email account, unless an appropriate request is lodged with IT manager and approved 	<input type="checkbox"/>
4.1.5g	<ul style="list-style-type: none"> ▪ Email message access limited to authorized personnel ▪ Staff do not share email passwords with other individuals 	<input type="checkbox"/>
4.1.5h	<ul style="list-style-type: none"> ▪ Internal mailing lists not distributed to non-staff members 	<input type="checkbox"/>
4.1.5i	<ul style="list-style-type: none"> ▪ Sender identity for emails not fogged/disguised 	<input type="checkbox"/>
4.1.5j	<ul style="list-style-type: none"> ▪ Sending of unsolicited bulk mail messages prohibited ▪ Users made aware of and comply with relevant spam/bulk email laws 	<input type="checkbox"/>
4.1.5k	<ul style="list-style-type: none"> ▪ Use of personal web based email permitted but users treat attachments/links as harmful and refrain from downloading or following using center laptops/desktops ▪ Personal email accounts not used for work purposes 	<input type="checkbox"/>
Email Accounts		
4.1.6	Emails are not permitted to be sent by one person using another person's email account (unless special dispensation obtained)	<input type="checkbox"/>
4.1.7	Email accounts identify users by real name or use pseudonyms easily attributable to actual users	<input type="checkbox"/>
Avoiding Malicious Email Content		
4.1.8	Executable files received via emails not executed on CGIAR center systems Patches and upgrades received via email not installed	<input type="checkbox"/>

Guideline Number	Guideline	Tick if center currently adheres to this guideline
4.1.9	Automatic previewing of HTML email disabled Automatic loading of pictures and active content disabled	<input type="checkbox"/>

7 DOCUMENT CONTROL

Version Control Log

Version	Description	Date
1.00	Final version prepared by SIFT Pty Ltd.	19 Jun 2009
1.10	First published edition	24 Aug 2009

Copyright & Legal

This guideline, prepared specifically for **Consultative Group for International Agricultural Research**, is the intellectual property of SIFT Pty Limited. When finalised, SIFT Pty Limited authorises CGIAR to reproduce or disseminate this guideline as necessary to further the aims and goals of CGIAR, under a Creative Commons Attribution-Noncommercial-Share Alike 2.5 Australia License

In no event shall SIFT Pty Limited be liable to anyone for special, incidental, collateral, or consequential damages arising out of the use of this information.

SIFT® is a Registered Trademark of SIFT Pty Ltd. Many designations used by manufacturers and sellers to distinguish their products are claimed as trademarks or other proprietary rights. Where designations appear, and when the editorial staff were aware of a claim, the designations have been shown. Other trademarks, registered trademarks, and service marks are the property of their respective owners.

Copyright © 2009 SIFT Pty Limited. Originated in Australia.

The first published version provided by SIFT Pty Limited, and future versions with modifications made by the CGIAR, as coordinated through the CGIAR ICTKM Program and the CGIAR Internal Auditing Unit, are being distributed by these Units in accordance with the terms of the above license, which can be found at <http://creativecommons.org/licenses/by-nc-sa/2.5/au/>.”